(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 791 877 B1

(12) FASCICULE DE BREVET EUROPEEN

(45) Date de publication et mention de la délivrance du brevet:
22.05.2002 Bulletin 2002/21

(51) Int Cl.[7]: **G06F 1/00**

(21) Numéro de dépôt: **97400398.0**

(22) Date de dépôt: **24.02.1997**

(54) Dispositif électronique délivrant une référence temporelle sûre pour la protection d'un logiciel

Elektronische Einrichtung zur Erzeugung einer sicheren Zeitreferenz zum Schutz einer Software

Electronic device providing a secure time reference for the protection of a program

(84) Etats contractants désignés:
DE GB

(30) Priorité: **26.02.1996 FR 9602340**

(43) Date de publication de la demande:
27.08.1997 Bulletin 1997/35

(73) Titulaire: **FRANCE TELECOM**
75015 Paris (FR)

(72) Inventeurs:
- **Arditti, David**
  92140 Clamart (FR)
- **Stoffel, Laurent**
  92130 Issy les Moulineaux (FR)

(74) Mandataire: **Dubois-Chabert, Guy et al**
BREVALEX
3, rue du Docteur Lanceraux
75008 Paris (FR)

(56) Documents cités:
WO-A-88/05941 **WO-A-92/12485**

- **SIEMENS MAGAZINE OF COMPUTERS & COMMUNICATIONS, (COM), vol. XIV, no. 5, Septembre 1986, MUNCHEN DE, pages 14-16, XP002018528 D. KRUSE: "Guarding the operating system"**

91 877 B1

Description

Domaine technique

[0001] La présente invention concerne un dispositif électronique délivrant une référence temporelle sûre pour la protection d'un logiciel, ce dispositif étant apte à être connecté à un ordinateur.

Etat de la technique antérieure

[0002] Tous les ordinateurs, du calculateur scientifique au modèle familial, possèdent une horloge interne et disposent ainsi d'une référence temporelle. De nombreux systèmes ou logiciels utilisent une telle référence temporelle pour différentes fonctionnalités non liées à leur protection. Une telle référence, en effet, est accessible et modifiable à l'aide du système d'exploitation de l'ordinateur concerné. Elle ne constitue donc pas une référence sûre.

[0003] Le piratage de logiciels (copies illicites, utilisation non conforme à la licence d'utilisation, ...) est très courant et constitue un préjudice important pour leurs éditeurs. De nombreux procédés de protection ont été utilisés à ce jour avec plus ou moins d'efficacité.

[0004] Il existe des versions de démonstration des logiciels, dans lesquelles certaines fonctionnalités importantes ne sont pas disponibles, mais aucune licence ne permet l'utilisation d'un logiciel avec toutes ses fonctionnalités pour une durée limitée. Ainsi la location ou la location-vente de logiciels, n'existe pas, car il n'y a pas de protection adaptée à de tels concepts.

[0005] De manière générale, il est très intéressant de disposer d'une référence temporelle sûre pour pouvoir concevoir de nouveaux mécanismes de protection des logiciels ou des systèmes.

[0006] A l'heure actuelle, les protections les plus sûres utilisent des moyens matériels associés aux logiciels, appelés de manière générique "dongles" ou "clés électroniques". Ces moyens matériels sont de petits objets externes (boîtiers, disquettes, ...) qui peuvent être connectés aux ordinateurs notamment par leurs ports série ou parallèle. Un dongle utilise des signaux particuliers, et/ou tout autre "secret" de fabrication, permettant au logiciel de s'assurer de la présence de celui-ci au cours d'une exécution et d'accepter un échange d'informations.

[0007] Malheureusement un dispositif peut être placé en coupure entre un ordinateur et un dongle pour analyser les signaux échangés. Aussi l'utilisation d'un dongle présente les inconvénients suivants :

- si le dongle envoie toujours les mêmes signaux, un faux dongle peut alors rejouer les signaux enregistrés en fonction de ceux émis par l'ordinateur ;
- si les signaux renvoyés par le dongle sont obtenus à partir de signaux émis par l'ordinateur comme résultat d'un calcul secret, alors le logiciel dispose du même secret dans son code pour vérifier l'authenticité des signaux transmis par le dongle ; par analyse du logiciel on peut alors retrouver ce secret pour réaliser ensuite un faux dongle.

[0008] Le comportement de dongles non cryptographiques peut ainsi être analysé à l'aide d'un dispositif en coupure ou par analyse du code du logiciel, pour être reproduit, par la suite, en l'absence de dongles.

[0009] Dans tous les cas de figure, les dongles actuels ne peuvent pas fournir de références temporelles, et donc a fortiori de références temporelles sûres.

[0010] De plus les dongles personnalisés pour un logiciel donné ne sont pas réutilisables par la suite pour un autre logiciel.

[0011] Certains systèmes ou logiciels distribués utilisent une référence de temps certifiée pour des fonctionnalités de sécurité. Une telle référence de temps est fournie par un ordinateur particulier (ou serveur), qui s'authentifie auprès des autres ordinateurs requérant son service. Mais cet ordinateur peut être "corrompu" par modification de son horloge interne, comme celle de n'importe quel autre ordinateur. Les autres ordinateurs lui font alors confiance mais l'heure fournie est inexacte. Un tel fonctionnement utilisé à des fins de sécurité interne à une organisation n'est pas adapté à la protection de logiciels. En effet il s'agit alors de protéger un logiciel d'une organisation contre l'utilisation illicite de celui-ci par d'autres organisations ou individus.

[0012] Un ordinateur fournissant une référence temporelle certifiée (serveur horloge) ne peut être considéré comme sûr par un éditeur de logiciel car cette machine appartient à l'utilisateur et pas à l'éditeur de logiciel.

[0013] Il existe des cartes à microprocesseur utilisant un algorithme pour permettre une authentification et une certification. Mais ces cartes, qui ne sont pas alimentées, ne peuvent pas disposer d'une horloge interne pour délivrer une heure certifiée.

[0014] Ainsi les dispositifs actuels ne permettent pas à un ordinateur de disposer d'une référence temporelle sûre pouvant être utilisée par un logiciel pour lutter contre le piratage.

[0015] L'objet de l'invention est de fournir une référence temporelle sûre dans un dongle, se connectant par exemple aux ports série ou parallèle d'un ordinateur, qu'un logiciel peut interroger pour s'assurer :

- de la satisfaction des conditions d'utilisation du logiciel ;
- de la présence du boîtier pour que le logiciel continue son exécution.

Exposé de l'invention

[0016] La présente invention concerne un dispositif électronique de vérification de l'utilisation licite d'un logiciel, apte à être connecté à un ordinateur, ledit dispositif comportant un microcontrôleur connecté à au moins

une mémoire, une horloge interne et une batterie interne dans lequel le microcontrôleur utilise un algorithme cryptographique asymétrique, qui repose sur l'utilisation d'une fonction de signature secrète et d'une fonction de vérification publique, et en ce que ledit dispositif contient la fonction de signature secrète, alors que le logiciel contient la fonction de vérification publique, caractérisé en ce qu'il comprend un compteur d'interrogations qui est incrémenté à chaque interrogation dudit dispositif, et un compteur de personnalisations qui permet de charger et de réinitialiser des "droits" d'utilisation, sous la forme de dates de début et/ou de fin de validité, de durée d'utilisation, etc..

[0017] Avantageusement le dispositif de l'invention est incorporé dans un boîtier scellé.

[0018] Avantageusement l'algorithme est un algorithme cryptographique asymétrique pris parmi les algorithmes suivants : RSA, FIAT-SHAMIR, DSA-DSS, GQ, -EL-GAMAL.

[0019] Avantageusement le dispositif de. l'invention permet de limiter l'utilisation du logiciel pour une période de validité (trois mois d'utilisation à partir de la première utilisation par exemple), de limiter l'utilisation du logiciel à un certain nombre d'utilisations, et à l'aide d'une implémentation idoine du logiciel de limiter son utilisation à une durée approximative (environ cinq cents heures, par exemple).

[0020] Le dispositif électronique de l'invention peut être rechargeable et permettre de racheter du temps d'utilisation a posteriori sur un simple appel téléphonique.

[0021] Le dispositif électronique de l'invention accepte une postpersonnalisation par des ordres certifiés, et est réutilisable

Brève description des dessins

[0022] La figure illustre le dispositif électronique de l'invention.

Exposé détaillé de modes de réalisation

[0023] le dispositif électronique de l'invention (10), tel que représenté sur la figure 1, est apte à être connecté aux ports série ou parallèle d'un ordinateur 11. Il est alimenté par une batterie interne (12), et contient notamment un microcontrôleur (13), connecté à des mémoires par exemple de type RAM (14) et ROM (15), et une horloge interne (16).

[0024] Ce dispositif peut être incorporé dans un boîtier scellé. Un tel boîtier peut, s'il est ouvert, se réinitialiser ou se détruire par tout moyen physique approprié, incorporé dans celui-ci. Un tel moyen physique connu de l'homme de l'art permet d'éviter une diffusion d'informations secrètes et rend incidemment toute utilisation ultérieure du logiciel impossible.

[0025] Le dispositif de l'invention est reconnu par le logiciel considéré à l'aide d'un mécanisme de signature reposant sur un algorithme cryptographique asymétrique, par exemple du type RSA (ou Rivest-Shamir-Adelman), Fiat-Shamir, DSA-DSS, GQ (ou Guillou-Quisquater), El Gamal, comme décrit dans de nombreux documents et notamment l'ouvrage intitulé "Applied Cryptography" de Bruce Scheiner (Edition John Wiley & Sons, 2ème édition, partie III, chapitres 19 à 21, pages 461 à 512, et partie IV).

[0026] Un algorithme de signature asymétrique repose sur l'utilisation d'une fonction de signature secrète et d'une fonction de vérification publique. La connaissance d'une fonction ne permet pas de connaître l'autre. Le dispositif contient la fonction secrète, alors que le logiciel à protéger contient la fonction publique qui ne permet qu'une vérification. Le logiciel à protéger ne contient donc aucun secret, car la connaissance de la fonction publique ne permet pas de signer des messages.

[0027] Toutes les interrogations du dispositif sont effectuées par le logiciel, qui lui envoie un nombre aléatoire pour éviter le rejeu, qui consiste pour une personne étrangère à observer une transaction quelconque entre deux dispositifs et à exécuter à nouveau cette transaction. Lorsque le dispositif répond, le nombre aléatoire est renvoyé avec la réponse à l'interrogation et la signature des données. Dans le cas particulier de l'algorithme RSA, la signature permet, par application de la fonction publique, de reconstituer les données.

[0028] L'observation des échanges entre l'ordinateur et le dispositif de l'invention n'est pas utilisable par une personne étrangère car ces échanges sont non déterministes et non rejouables (présence de l'aléa).

[0029] Si on prend l'exemple de l'algorithme RSA, S étant la fonction de signature secrète, P la fonction de vérification publique, a un nombre aléatoire, H l'heure (et la date), / indiquant l'opérateur concaténation, on a la signature : c = S (H/a), et la fonction de vérification publique P(c) = H/a.

[0030] Lorsque le dispositif de l'invention est interrogé, il ne répond que si les modalités prévues sont toutes satisfaites (date de fin de validité non atteinte, durée d'utilisation non atteinte, . .).

[0031] On va, à présent, considérer le cycle de vie d'un boîtier ; lors de la fabrication, l'éditeur du logiciel réalise :

- l'introduction du numéro de série du boîtier ;
- l'introduction de la fonction secrète asymétrique de l'éditeur ;
- la mise à l'heure de l'horloge ;
- l'initialisation du compteur d'interrogations (17) : celui-ci, qui est incrémenté à chaque interrogation du boîtier, permet de faire une correspondance entre le nombre d'utilisations du logiciel et une certaine durée d'utilisation du logiciel ; ce qui présuppose une implémentation appropriée du logiciel ;
- l'introduction de la date de début de validité, de la date de fin de validité, de la durée d'utilisation...

[0032] Ces données ne sont plus modifiés jusqu'à une réinitialisation complète du boîtier (réutilisation). Elles seront appelées par la suite "droits d'utilisation".

[0033] Les procédures de personnalisation et de postpersonnalisation sont mises en oeuvre avant/pendant la vente (personnalisation) du logiciel et éventuellement en cours d'utilisation (postpersonnalisation) pour mettre à jour les données relatives à l'utilisation du logiciel.

[0034] Si le dispositif de l'invention est utilisé comme une horloge certifiée sans limitation de durée, des valeurs particulières sont attribuées aux registres correspondant à la date de fin de validité et à la durée d'utilisation.

[0035] Pour réaliser les échanges d'information le dispositif de l'invention accepte des ordres d'initialisation/mise à jour des droits. Ces ordres sont certifiés par une procédure classique. Les certificats sont calculés par l'éditeur de logiciel grâce à un algorithme symétrique et à une clé secrète, qui donne son pouvoir d'attribution des droits à l'éditeur. Cette clé est contenue dans ledit dispositif et partagée avec l'éditeur. Chaque boîtier possède une clé symétrique propre. L'éditeur est en mesure de retrouver toutes ces clés par un procédé classique de diversification d'une clé mère à partir du numéro de série du boîtier.

[0036] Un fichier de personnalisation contient les droits et leur certificat. Il est livré à l'utilisateur lors de l'achat du logiciel ou d'une mise à jour des droits. Ce fichier ne contient aucune information secrète.

[0037] Un tel fonctionnement permet une gestion des droits en absolu (date, nombre d'utilisations). Pour gérer ces éléments de façon incrémentale (ajouter 100 utilisations par exemple) il faut se prémunir contre le rejeu de la postpersonnalisation. Dans ce but, le dispositif possède un compteur de personnalisations (18).

[0038] Initialisé à 0, ce compteur est pris en compte dans le calcul des certificats. Le boîtier accepte la mise à jour des droits si la valeur transmise est strictement supérieure à la valeur courante. La valeur transmise est alors affectée au compteur.

[0039] La réinitialisation totale du boîtier, qui permet sa réutilisabilité, n'a pas besoin d'être certifiée.

Revendications

1. Dispositif électronique de vérification de l'utilisation licite d'un logiciel, apte à être connecté à un ordinateur (11), ledit dispositif comportant un microcontrôleur (13) connecté à au moins une mémoire (14, 15), une horloge interne (16) et une batterie interne (12), dans lequel le microcontrôleur utilise un algorithme cryptographique asymétrique, qui repose sur l'utilisation d'une fonction de signature secrète et d'une fonction de vérification publique, ledit dispositif contenant la fonction de signature secrète, alors que le logiciel contient la fonction de vérification publique, **caractérisé en ce qu'**il comprend un compteur d'interrogations (17) qui est incrémenté à chaque interrogation dudit dispositif, et un compteur de personnalisations (18) qui permet de charger et de réinitialiser des "droits" d'utilisation, sous la forme de dates de début et/ou de fin de validité, de durée d'utilisation.

2. Dispositif selon la revendication 1, **caractérisé en ce que** ledit dispositif est connecté audit ordinateur par ses ports série ou parallèle.

3. Dispositif selon la revendication 1, **caractérisé en ce qu'**il est incorporé dans un boîtier scellé.

4. Dispositif selon la revendication 1, **caractérisé en ce que** l'algorithme est un algorithme cryptographique asymétrique pris parmi les algorithmes suivants : RSA, FIAT-SHAMIR, DSA-DSS, GQ, EL-GAMAL.

Patentansprüche

1. Elektronische Vorrichtung zur Überprüfung der rechtmäßigen Verwendung von Software, die mit einem Computer (11) verbunden werden kann, wobei die Vorrichtung einen Mikro-Controller (13) umfaßt, der mit mindestens einem Speicher (14,15), einem internen Taktgeber (16) und einer internen Batterie (12) verbunden ist, wobei der Mikro-Controller einen asymmetrischen Kryptographiealgorithmus anwendet, der auf der Verwendung einer geheimen Signaturfunktion und einer öffentlichen Verifizierungsungsfunktion beruht, wobei die Vorrichtung die geheime Signaturfunktion enthält, während die Software die öffentliche Verifizierungsungsfunktion enthält, **dadurch gekennzeichnet, daß** sie (die Vorrichtung) einen Abfragezähler (17) umfaßt, der bei jeder Abfrage der Vorrichtung fortgeschrieben wird, sowie einen Personalisierungszähler (18), der ein Laden und Re-Initialisieren von Benutzungs-"Rechten" in Form von Anfangs- und/oder Enddaten der Gültigkeit, der Benutzungsdauer ermöglicht.

2. Vorrichtung nach Anspruch 1, **dadurch gekennzeichnet, daß** die Vorrichtung mit dem Computer über seine seriellen oder parallelen Ports verbunden ist.

3. Vorrichtung nach Anspruch 1, **dadurch gekennzeichnet, daß** sie in ein verslegeltes Gehäuse aufgenommen ist.

4. Vorrichtung nach Anspruch 1, **dadurch gekennzeichnet, daß** der Algorithmus ein asymmetrischer Kryptographiealgorithmus ist, der unter den folgen-

den Algorithmen ausgewählt ist: RSA, FIAT-SHAMIR, DSA-DSS, GQ, EL-GAMAL.

Claims

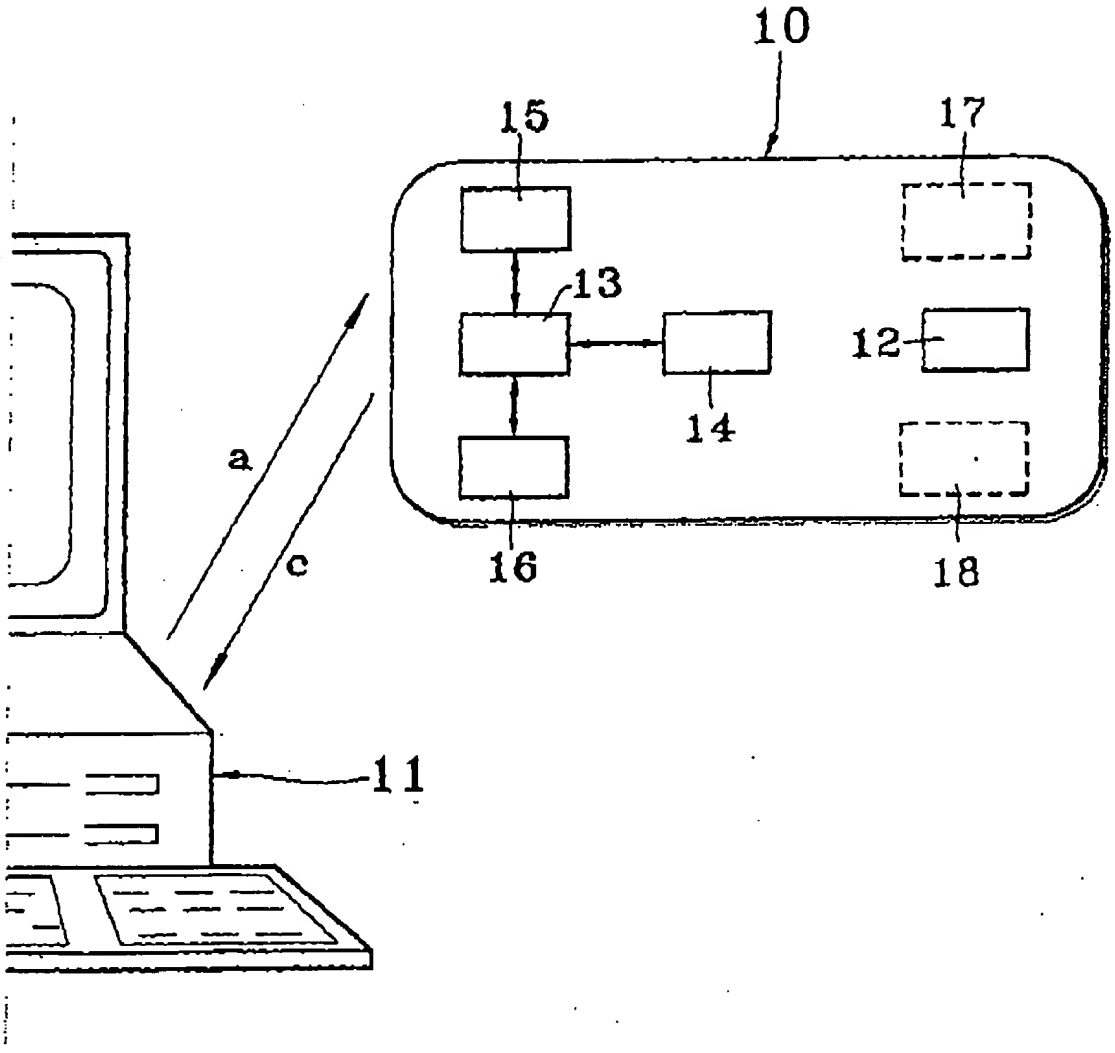
1. Electronic device for verifying the lawful use of a program, adapted to be connected to a computer (11), the said device comprising a microprocessor (13) connected to at least one memory (14, 15), an internal clock (16) and an internal battery (12), in which the microprocessor uses an asymmetric cryptographic algorithm, which is based on the use of a secret signature function and a public verification function, the said device containing the secret signature function, whereas the program contains the public verification function, **characterised in that** it comprises an interrogation counter (17) which is incremented for each interrogation of the said device, and a personalisation counter (18) which allows the loading and the re-initialisation of the rights of use, in the form of start and end dates of validity, of the length of use.

2. Device according to claim 1, **characterised in that** the said device is connected to the said computer by serial or parallel ports.

3. Device according to claim 1, **characterised in that** it is incorporated in a sealed box.

4. Device according to claim 1, **characterised in that** the algorithm is an asymmetric cryptographic algorithm chosen from the following algorithms: RSA, FIAT-SHAMIR, DSA-DSS, GQ, EL-GAMAL.

FIG. 1



Machine Translation of Text of EP 0791877

Technical domain The presents invention concerns an electronic device delivering a sure temporal reference for the protection of a software, this device being capable of be connected to a computer.

State of the previous technique All the computers, scientific calculator to the family model, possess an internal clock and dispose thus of a temporal reference. Many systems or software use temporal such a reference for different non secured functionalities to their protection. Such a reference, in fact, accessible east and modifiable to the assistance of the operating system of the concerned computer. She does not constitute therefore a sure reference. The piratage of software (illicit copies, non usage in accordance with the usage license,...) very current east and constitutes an important harm for their editors. Many protection procedures were used to this day with more or less than effectiveness. There exist the demonstration versions of software, in which ones certain important functionalities are not available, but no license allows the usage of a software with all its functionalities for a limited length. Thus the housing or the housing sale of software, does not exist, for there is not adapted protection to such concepts. In a general way, it is very interesting to have access to a sure temporal reference to be able to conceive again protection mechanisms of software or systems. At the present time, the protections more sure use material means associated to software, called in a generic way "dongles" or "electronic keys". These material means are small external objects (cases, diskettes,...) that can be connected to the computers notably by their harbors series or parallel. A dongle uses special signals, and or all other "secret" of manufacture, allowing the software to assure itself presence of this one during an execution and to accept an exchange of information. Unfortunately a device can be placed in cut between a computer and a dongle to analyze the exchanged signals. Also the usage of a dongle presents the following inconveniences:

• if the dongle always sends them same signals, a false dongle then can replay the recorded signals according to those emitted by the computer; • if the signals sent back by the dongle are obtained from signals emitted by the computer as result of a secret calculation, then software has access to the same secret in his code to verify the authenticity of the signals transmitted by the dongle; byOne then can rediscover this secret to realize next a false dongle.

The non cryptographic dongles behavior can thus be analyzed to the assistance of a device in cut or by analyzes code of software, for be reproduced, by the continuation, in the absence of dongles. In any case of face, the current dongles cannot furnish temporal references, and therefore has fortiori of sure temporal references. Of more the dongles personnalisés for a given software are not réutilisables by the continuation for another software. Certain systems or distributed software use a time reference certified for security functionalities. Times such a reference is furnished by a special computer (or waiter), that authenticates itself with the other computers requiring his service. But this computer can be "corrupt" by modification of his internal clock, as the one of other any computer. The other computers do him then confidence but the furnished hour is inexact. Used such a functioning to security ends internal to an organization is not adapted to the protection of software. In fact it is a matter then to protect a software of an organization against the illicit usage of this one by of other organizations or individuals. A computer furnishing a temporal certified

reference (waiter clock) cannot be considered as sure by a software editor for this machine belongs to the user and to the software editor. There exist the cards to microprocesseur using an algorithm to allow an authentification and a certification. But these cards, that are not supplied, cannot have access to an internal clock to deliver a certified hour. Thus the current devices do not allow a computer to have access to a sure temporal reference being able to be to have used by a software to fight against the piratage. The object of the invention is to furnish a sure temporal reference in a dongle, being connected for example to the harbors series or parallel of a computer, that a software can question to assure itself: - satisfaction of the usage conditions of software; - presence of the case for that software continues his execution. Exposed invention presents It invention concerns an electronic device of verification of the usage licite of a software, capable of be connected to a computer, the aforementioned device behaving a microcontrôleur connected to at least a memory, an internal clock and an internal battery in which the microcontrôleur uses an assymetrical cryptographic algorithm, that rests on the usage of a signature function secret and of a function ofDevice contains the signature function secret, while software contains the verification function public, characterized in this that it understands a meter of interrogations that is incrémenté to every interrogation dudit device, and a meter of personalizations that allows loading and of réinitialiser of the "rights" of usage, under the form of starting dates and or of validity end, of usage length, etc.. Advantageous the device of the invention is incorporated in a case seal. Advantageous algorithm is an assymetrical cryptographic algorithm take among following algorithms: RSA, fiat-shamir, dsa-dss, GQ, - EL-GAMAL. Advantageous the device of. the invention allows limiting the usage of the software for a
validity period (three months of usage from the first usage for example), to limit the usage of the software to a number of usages, and to the assistance of an implémentation idoine of the software to limit his usage to an approximate length (about five hundred hours, for example). The electronic device of the invention can be rechargeable and allow repurchasing usage time has posteriori on a simple telephone call. The electronic device of the invention accepts a postpersonnalisation by certified orders, and is réutilisable

Brief description of the drawings figures It illustrates the electronic device of the invention.

Exposed detailed realization methods the electronic device of the invention (10), such as represented on the figure 1, capable of east to be connected to the harbors series or parallel of a computer 11. It is supplied by an internal battery (12), and contains notably a microcontrôleur (13), connected to memories for example of type RAM (14) and ROM (15), and an internal clock (16). This device can be incorporated in a case seal. Such a case can, if it is opened, itself réinitialiser or to destroy itself by all fitting physical means, incorporated in this one. A such physical average known man of the art allows avoiding a broadcasting of secret information and returns in passing all later usage of impossible software. The device of the invention is recognized by considered software to the assistance of a signature mechanism resting on a cryptographic assymetrical algorithm, for example type RSA (or Rivest-Shamir-Adelman), fiat-shamir, dsa-dss, GQ (or guillou-quisquater), El Gamal, as describes in many documents and notably the entitled work "Applied Cryptography" of Bruce Scheiner (Edition John Wiley & Sounds, 2nd edition, left III, chapters 19 to 21, orderlies 461 to. A signature algorithm assymetrical rests on the usage of a signature function secret and of a verification function public. The knowledge of a function does not allow knowing the other. The device contains the secret function, while the software to

protect contains the public function that allows only a verification. The software to protect does not contain therefore no secret, for the knowledge of the public function allows signing messages. All the interrogations of the device are carried out by software, that sends him a random number to avoid the rejeu, that consists for a foreign person to observe a transaction any between two devices and to execute again this transaction. When the device replies, the random number is sent back with the response to the interrogation and the signature of the data. In the special case of algorithm RSA, the signature allows, by application of the public function, to restore the data. The observation of the exchanges between the computer and the device of the invention is not usable by a foreign person for these exchanges are deterministic non and non-rejouables (presence of hazard). If one takes the example of algorithm RSA, S being the signature function secret, P the verification function public, has a random number, H the hour (and the date), / indicating the operator concatenation, one has the signature: c = S (h/a), and the verification function public P(c) (P(c)). When the device of the invention is questioned, it replies only if the foreseen methods all are satisfied (dates back to non attained validity end, lasted of non attained usage,. .). One goes, at present, consider the life cycle of a case; at the time of the manufacture, the editor of software realizes:

- the introduction of the number of series of the case; - the introduction of the assymetrical secret function of the editor; - the placement per hour of the clock; - the initialisation of the meter of interrogations (17) : this one, that is incrémenté to every interrogation of the case, allows doing a correspondence between the number of usages of software and a certain usage length of software; this that presupposes The introduction of the validity starting date, of the date back to validity end, length d'utilisation...

These data more are not modified until a réinitialisation completes case (réutilisation). They will be called by the continuation "usage rights". The personalization procedures and of postpersonnalisation are implemented before during the sale (personalization) software and eventually in usage course (postpersonnalisation) to update them given relating to the usage of software. If the device of the invention is used as a certified clock without length limitation, special values are attributed to the registers corresponding to the date back to validity end and to the usage length. To realize the information exchanges the device of the invention accepts on the order of initialisation/ updated rights. These orders are certified by a classical procedure. The certificates are calculated by the software editor thanks to a symmetrical algorithm and to a secret key, that gives his granting strength of the rights to the editor. This key is contained in the aforementioned device and divided with the editor. Every case possesses a clean symmetrical key. The editor is in a position to rediscover all these keys by a classical procedure of diversification of a key mother from the number of series of the case. A personalization file contains the rights and their certificate. It is delivered to the user at the time of the purchase of software or of an update rights. This file does not contain no secret information. Such a functioning allows a management of the rights in absolute (dates, number of usages). To manage these elements in a manner incrémentale (to add 100 usages for example) it is necessary to caution himself against the rejeu of the postpersonnalisation. With this aim, the device possesses a meter of personalizations (18). Initialized to 0, this meter is taken into account in the calculation of the certificates. The case accepts the update rights if the transmitted value is strictly superior to the value running. The transmitted value then is affected to the meter. The total réinitialisation of the case, that allows his réutilisabilité, does not need to be certified.